CLAIMS

1. A system for encrypting and decrypting data formed of a number of bytes using an encryption algorithm, comprising:

a system bus;

an encryption accelerator arranged to execute the encryption algorithm coupled to the system bus;

a system memory coupled to the system bus arranged to store a secret key array associated with the data; and

a central processing unit coupled to the system bus wherein encryption accelerator uses substantially no central processing unit resources to execute the encryption algorithm.

2. A system as recited in claim 1, wherein the encryption accelerator includes a state memory that includes a plurality of state memory values each of which is associated with a particular state memory location.

3. A system as recited in claim 1, further comprising:

a storage unit coupled to the encryption accelerator arranged to store at least a portion of the data to be encrypted wherein the storage unit is in temporal proximity to the encryption accelerator thereby improving system performance.

4. A system as recited in claim 1, wherein the encryption algorithm is an ARCFOUR encryption algorithm.

5. A system as recited in claim 4, wherein the system encrypts the data using the ARCFOUR algorithm by,

initializing the state memory with an incrementing pattern, and

shuffling each of the plurality of state memory values from an original state memory location to a corresponding shuffled state memory location based upon the secret key array such that the shuffled state memory location is only known if the secret key array is known.

6. A system as recited in claim 5, wherein the shuffling operation comprises:

transferring the secret key array and an associated message data length into the encryption accelerator by way of the system bus thereby preserving central processing unit resources.

7. A system as recited in claim 6, wherein the shuffling is performed on the fly concurrently with the transferring.

8. A system as recited in claim 7, further comprising:

upon completion of the shuffling, the data to be encrypted is transferred to the encryption accelerator by way of the system bus such that for each byte of the data the encryption accelerator produces a corresponding byte from the state memory that is exclusive OR'd with the byte of data to be encrypted.

9. A system as recited in claim 1, further comprising an external memory coupled to the state memory arranged to store selected state memory values.

10. A system as recited in claim 9, wherein the encryption accelerator is selectively operable in an Initial Mode and a Continuation mode wherein in the Initial Mode the system operates in a sequential manner whereas in the continuation mode the state memory is reloaded with the stored state memory values.

11. An efficient encryption accelerator arranged to encrypt and decrypt data formed of a number of bytes using an encryption algorithm, comprising:

a combinational logic block arranged to perform a pre-determined logic operation on selected input values;

a state memory array coupled to the combinational logic block arranged to store a plurality of state memory values;

a state machine coupled to the combinational logic block and the state memory array that directs,

storing of an incrementing pattern in the state memory array,

performing a shuffling operation on the fly while concurrently retrieving a secret key associated with the data, wherein the shuffling operation includes moving each of the plurality of state memory values based upon the secret key,

byte-wise transferring the data to the combinational logic block as a first input value, and

transferring a corresponding state memory value to the combinational logic as a second input value;

logically operating on the first and the second input values by the combinational logic to form an encrypted data byte; and

outputting the encrypted data byte.

12. An accelerator as recited in claim 12, wherein the encryption algorithm is an ARCFOUR algorithm.

13. An accelerator as recited in claim 12, wherein the accelerator is coupled to a system memory arranged to store the secret key and wherein the accelerator is coupled to a CPU in such a way that the accelerator operates to encrypt the data so as to preserve CPU resources.

14. An accelerator as recited in claim 13, wherein the CPU is coupled to the accelerator and the system memory by way of a system bus.

15. An accelerator as recited in claim 11, further comprising an input latch coupled to the state machine, the state memory array, and the combinational logic block arranged to store the data to be encrypted.

16. An accelerator as recited in claim 11, further comprising an output latch coupled to the state machine, the state memory array, and the combinational logic block arranged to store the encrypted data.

17. An accelerator as recited in claim 11, wherein the logic function is an exclusive OR logic function.

18. An accelerator as recited in claim 14, wherein the data to be encrypted is passed to the input latch by way of the system bus as directed by the CPU.

19. An accelerator as recited in claim 18, wherein the encrypted data is passed to external circuitry as directed by the CPU by way of an output node coupled to the system bus.

20. An accelerator as recited in claim 11, wherein the accelerator further includes a first index counter and a second index counter each of which is connected to and directed by the state machine.

21. An accelerator as recited in claim 11, wherein the accelerator is included in a computing device.

22. An accelerator as recited in claim 21, wherein the computing device is connected to an interconnected network of computing devices, wherein the accelerator encrypts a sent message sent to at least one of the network of computing devices and wherein the accelerator decrypts a received message from at least one of the network of computing devices.